UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

NOTICE OF ALLOWANCE AND FEE(S) DUE

29989 7590 02/01/2010

HICKMAN PALERMO TRUONG & BECKER, LLP
2055 GATEWAY PLACE
SUITE 550
SAN JOSE, CA 95110

EXAMINER	
KIM, PAUL	
ART UNIT	PAPER NUMBER
2169	

DATE MAILED: 02/01/2010

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/698,498	10/30/2003	Sanjay Aiyagari	50325-0805	9591

TITLE OF INVENTION: ROLE-BASED ACCESS CONTROL ENFORCED BY FILESYSTEM OF AN OPERATING SYSTEM

APPLN. TYPE	SMALL ENTITY	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	NO	$1510	$0	$0	$1510	05/03/2010

THE APPLICATION IDENTIFIED ABOVE HAS BEEN EXAMINED AND IS ALLOWED FOR ISSUANCE AS A PATENT. PROSECUTION ON THE MERITS IS CLOSED. THIS NOTICE OF ALLOWANCE IS NOT A GRANT OF PATENT RIGHTS. THIS APPLICATION IS SUBJECT TO WITHDRAWAL FROM ISSUE AT THE INITIATIVE OF THE OFFICE OR UPON PETITION BY THE APPLICANT. SEE 37 CFR 1.313 AND MPEP 1308.

THE ISSUE FEE AND PUBLICATION FEE (IF REQUIRED) MUST BE PAID WITHIN THREE MONTHS FROM THE MAILING DATE OF THIS NOTICE OR THIS APPLICATION SHALL BE REGARDED AS ABANDONED. THIS STATUTORY PERIOD CANNOT BE EXTENDED. SEE 35 U.S.C. 151. THE ISSUE FEE DUE INDICATED ABOVE DOES NOT REFLECT A CREDIT FOR ANY PREVIOUSLY PAID ISSUE FEE IN THIS APPLICATION. IF AN ISSUE FEE HAS PREVIOUSLY BEEN PAID IN THIS APPLICATION (AS SHOWN ABOVE), THE RETURN OF PART B OF THIS FORM WILL BE CONSIDERED A REQUEST TO REAPPLY THE PREVIOUSLY PAID ISSUE FEE TOWARD THE ISSUE FEE NOW DUE.

HOW TO REPLY TO THIS NOTICE:

I. Review the SMALL ENTITY status shown above.

If the SMALL ENTITY is shown as YES, verify your current SMALL ENTITY status:

A. If the status is the same, pay the TOTAL FEE(S) DUE shown above.

B. If the status above is to be removed, check box 5b on Part B - Fee(s) Transmittal and pay the PUBLICATION FEE (if required) and twice the amount of the ISSUE FEE shown above, or

If the SMALL ENTITY is shown as NO:

A. Pay TOTAL FEE(S) DUE shown above, or

B. If applicant claimed SMALL ENTITY status before, or is now claiming SMALL ENTITY status, check box 5a on Part B - Fee(s) Transmittal and pay the PUBLICATION FEE (if required) and 1/2 the ISSUE FEE shown above.

II. PART B - FEE(S) TRANSMITTAL, or its equivalent, must be completed and returned to the United States Patent and Trademark Office (USPTO) with your ISSUE FEE and PUBLICATION FEE (if required). If you are charging the fee(s) to your deposit account, section "4b" of Part B - Fee(s) Transmittal should be completed and an extra copy of the form should be submitted. If an equivalent of Part B is filed, a request to reapply a previously paid issue fee must be clearly made, and delays in processing may occur due to the difficulty in recognizing the paper as an equivalent of Part B.

III. All communications regarding this application must give the application number. Please direct all communications prior to issuance to Mail Stop ISSUE FEE unless advised to the contrary.

IMPORTANT REMINDER: Utility patents issuing on applications filed on or after Dec. 12, 1980 may require payment of maintenance fees. It is patentee's responsibility to ensure timely payment of maintenance fees when due.

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), to: Mail **Mail Stop ISSUE FEE**
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
or Fax (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

29989 7590 02/01/2010

HICKMAN PALERMO TRUONG & BECKER, LLP
2055 GATEWAY PLACE
SUITE 550
SAN JOSE, CA 95110

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission

I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being facsimile transmitted to the USPTO (571) 273-2885, on the date indicated below.

(Depositor's name)

(Signature)

(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/698,498	10/30/2003	Sanjay Aiyagari	50325-0805	9591

TITLE OF INVENTION: ROLE-BASED ACCESS CONTROL ENFORCED BY FILESYSTEM OF AN OPERATING SYSTEM

APPLN. TYPE	SMALL ENTITY	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	NO	$1510	$0	$0	$1510	05/03/2010

EXAMINER	ART UNIT	CLASS-SUBCLASS
KIM, PAUL	2169	707-009000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).

☐ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.

☐ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-02 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list

(1) the names of up to 3 registered patent attorneys or agents OR, alternatively,

(2) the name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.

1 _____

2 _____

3 _____

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document has been filed for recordation as set forth in 37 CFR 3.11. Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE

(B) RESIDENCE: (CITY and STATE OR COUNTRY)

Please check the appropriate assignee category or categories (will not be printed on the patent) : ☐ Individual ☐ Corporation or other private group entity ☐ Government

4a. The following fee(s) are submitted:

☐ Issue Fee

☐ Publication Fee (No small entity discount permitted)

☐ Advance Order - # of Copies _____

4b. Payment of Fee(s): **(Please first reapply any previously paid issue fee shown above)**

☐ A check is enclosed.

☐ Payment by credit card. Form PTO-2038 is attached.

☐ The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment, to Deposit Account Number _____ (enclose an extra copy of this form).

5. **Change in Entity Status** (from status indicated above)

☐ a. Applicant claims SMALL ENTITY status. See 37 CFR 1.27.

☐ b. Applicant is no longer claiming SMALL ENTITY status. See 37 CFR 1.27(g)(2).

NOTE: The Issue Fee and Publication Fee (if required) will not be accepted from anyone other than the applicant; a registered attorney or agent; or the assignee or other party in interest as shown by the records of the United States Patent and Trademark Office.

Authorized Signature _____ Date _____

Typed or printed name _____ Registration No. _____

This collection of information is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P O Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/698,498	10/30/2003	Sanjay Aiyagari	50325-0805	9591

29989 7590 02/01/2010

HICKMAN PALERMO TRUONG & BECKER, LLP
2055 GATEWAY PLACE
SUITE 550
SAN JOSE, CA 95110

EXAMINER	
KIM, PAUL	
ART UNIT	PAPER NUMBER
2169	

DATE MAILED: 02/01/2010

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)
(application filed on or after May 29, 2000)

The Patent Term Adjustment to date is 444 day(s). If the issue fee is paid on the date that is three months after the mailing date of this notice and the patent issues on the Tuesday before the date that is 28 weeks (six and a half months) after the mailing date of this notice, the Patent Term Adjustment will be 444 day(s).

If a Continued Prosecution Application (CPA) was filed in the above-identified application, the filing date that determines Patent Term Adjustment is the filing date of the most recent CPA.

Applicant will be able to obtain more detailed information by accessing the Patent Application Information Retrieval (PAIR) WEB site (http://pair.uspto.gov).

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Customer Service Center of the Office of Patent Publication at 1-(888)-786-0101 or (571)-272-4200.

Notice of Allowability	Application No.	Applicant(s)	
	10/698,498	AIYAGARI ET AL.	
	Examiner	Art Unit	
	PAUL KIM	2169	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *Notice of Appeal Filed on 10 November 2009*.

2. ☒ The allowed claim(s) is/are *1, 2, 4, 7, 9-13, 16, 18-19, 39-40, 42, 45, 47-51, 54, and 56-57*.

3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application
6. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____ .
7. ☒ Examiner's Amendment/Comment
8. ☐ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

/Tony Mahmoudi/
Supervisory Patent Examiner, Art Unit 2169

Examiner's Amendment

1. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Daniel Ledesma on 28 January 2010.

2. The application has been amended as follows:

=====

1. (currently amended) A computer-implemented method for controlling access to a resource of a plurality of resources, the method comprising the steps of:

one or more processors creating and storing in a filesystem of an Operating System a plurality of files that each represents a different resource of the plurality of resources;

the one or more processors assigning an access value to a file attribute of a file that represents the resource, wherein the file attribute is used by the Operating System to manage file access, wherein the access value corresponds to a combination of a particular role and the resource;

the one or more processors receiving user-identifying information from a user requesting access to the resource, wherein the user-identifying information comprises a role associated with the user, wherein the role is determined from a user identifier

uniquely associated with the user and from a group identifier associated with a group that includes the user;

the one or more processors receiving a resource identifier associated with the resource;

the one or more processors creating an access identifier based on the user-identifying information and the resource identifier, wherein the access identifier is formatted as a file attribute that is used by the Operating System to manage file access;

wherein the step of creating an access identifier based on the user-identifying information and the resource identifier comprises formatting the access identifier as a group identifier file attribute;

the one or more processors calling the Operating System to perform a file operation on the file, wherein calling the Operating System includes providing the access identifier to the Operating System; [[and]]

wherein the step of calling the Operating System to perform an operation on the file representing the resource comprises:

assigning the access identifier to a group identifier attribute of an Operating System process; and

calling an Operating System routine from the Operating System process to perform the operation on the file representing the resource;

the one or more processors granting the user access to the resource only when the Operating System call successfully performs the file operation, wherein the Operating System call successfully performs the file operation if the access identifier matches the access value;

wherein the file operation on the file representing the resource is selected from a group consisting of opening the file, closing the file, deleting the file, reading from the file, writing to the file, executing the file, appending to the file, reading a file attribute, and writing a file attribute;

reading a permission bit associated with the file representing the resource, wherein the permission bit corresponds to the operation performable on the file representing the resource;

based on the operation on the file indicated by the permission bit, determining a resource operation that is performable on the resource; and

granting the user the privilege of performing the resource operation on the resource only when the permission bit allows the operation to be performed on the file representing the resource.

2. (original) A method as recited in Claim 1, wherein the access identifier comprises:

a first set of bits for storing a role identifier, wherein the role identifier is associated with the role; and

a second set of bits for storing the resource identifier.

3. (canceled)

4. (original) A method as recited in Claim 1, wherein the step of calling the Operating System to perform an operation on the file representing the resource comprises

comparing the access identifier to an identifier included in an Access Control List file attribute associated with the file representing the resource, wherein the Access Control List file attribute includes the identifiers of all users and all groups of users allowed to access the file representing the resource.

5. (canceled)

6. (canceled)

7. (previously presented) A method as recited in Claim 1, the method further comprising the steps of:

opening the file representing the resource;

reading from the file representing the resource a permission indicator associated with a resource operation; and

enabling the user to perform the resource operation on the resource only when the permission indicator indicates that the user is allowed to perform the resource operation on the resource.

8. (canceled)

9. (previously presented) A method as recited in Claim 1, wherein the file attribute used by the Operating System to manage file access is a group identifier file attribute.

10. (currently amended) A computer-implemented method for controlling access to a resource of a plurality of resources, the method comprising the steps of:

one or more processors assigning an access value to a group identifier file attribute of a file that represents the resource, wherein the group identifier file attribute is used by the Operating System to manage file access, wherein the access value is uniquely determined by a combination of a particular role and the resource;

the one or more processors receiving a user identifier from a user requesting access to the resource, wherein the user identifier is uniquely associated with the user;

the one or more processors receiving a group identifier associated with a group to which the user belongs;

the one or more processors based on the user identifier and the group identifier, determining a role associated with the user, wherein a role identifier is uniquely associated with the role;

the one or more processors receiving a resource identifier associated with the resource, wherein each resource of the plurality of resources is represented by a different file stored in a filesystem of an Operating System;

the one or more processors constructing an access identifier on the basis of the role identifier and the resource identifier, wherein the access identifier conforms to the format of a group identifier file attribute that is used by the Operating System to manage file access;

the one or more processors making an Operating System call to perform a file operation on the file representing the resource, wherein the Operating System call uses the access identifier to gain access to the file representing the resource; and

the one or more processors granting the user access to the resource only when the Operating System call successfully performs the file operation on the file representing the resource, wherein the Operating System call successfully performs the file operation if the access identifier matches the access value;

wherein the file operation on the file representing the resource is selected from a group consisting of opening the file, closing the file, deleting the file, reading from the file, writing to the file, executing the file, appending to the file, reading a file attribute, and writing a file attribute;

reading a permission bit associated with the file representing the resource, wherein the permission bit corresponds to a file operation performable on the file representing the resource;

based on the file operation indicated by the permission bit, determining a resource operation that is performable on the resource; and

granting the user the privilege of performing the resource operation on the resource only when the permission bit allows the file operation to be performed on the file representing the resource.

11. (original) A method as recited in Claim 10, wherein the access identifier comprises:

a first set of bits for storing the role identifier, wherein the role identifier represents a bitmap, each bit of the bitmap uniquely associated with a role of the user; and

a second set of bits for storing the resource identifier.

12. (previously presented) A method as recited in Claim 10, wherein the step of making an Operating System call to perform an operation on the file representing the resource comprises:

storing the group identifier value of a group identifier attribute of an Operating System process;

assigning the access identifier to the group identifier attribute of the Operating System process;

calling an Operating System routine from the Operating System process to perform the operation on the file representing the resource, wherein the operation on the file representing the resource is performed only when the value of the group identifier attribute of the Operating System process matches the value of the group identifier file attribute of the file representing the resource; and

resetting the group identifier attribute of the Operating System process to the stored group identifier value.

13. (original) A method as recited in Claim 10, wherein the step of making an Operating System call to perform an operation on the file representing the resource comprises comparing the access identifier to an identifier included in an Access Control List file

attribute associated with the file representing the resource, wherein the Access Control List file attribute includes the identifiers of all users and all groups of users allowed to access the file representing the resource.

14. (canceled)

15. (canceled)

16. (previously presented) A method as recited in Claim 10, the method further comprising the steps of:

opening the file representing the resource;

reading from the file representing the resource a permission indicator associated with a resource operation; and

granting the user the privilege of performing the resource operation on the resource only when the permission indicator indicates that the user is allowed to perform the resource operation on the resource.

17. (canceled)

18. (currently amended) A system for controlling access to a resource, of a plurality of resources, connected to a network, the system comprising:

a client host capable of accessing the resource in response to a request for access from a user;

one or more processors executing an Operating System, wherein the Operating System operatively controls a filesystem that includes a number of files; and

a computer readable medium having stored therein an Application Programming Interface, wherein the Application Programming Interface is logically interposed between the client host and the Operating System and comprises one or more routines including routines which, when executed by the one or more processors, cause the one or more processors to perform the steps of:

creating and storing in the filesystem a plurality of files that each represents a different resource of the plurality of resources;

assigning an access value to a file attribute of a file that represents the resource, wherein the file attribute is used by the Operating System to manage file access, wherein the access value corresponds to a combination of a particular role and the resource;

receiving user-identifying information from the user requesting access to the resource, wherein the user-identifying information comprises a role associated with the user, wherein the role is determined from a user identifier uniquely associated with the user and from a group identifier associated with a group that includes the user;

receiving a resource identifier associated with the resource;

creating an access identifier based on the user-identifying information and the resource identifier, wherein the access identifier is formatted as a file attribute that is used by the Operating System to manage file access;

wherein the step of creating an access identifier based on the user-identifying information and the resource identifier comprises formatting the access identifier as a group identifier file attribute;

calling the Operating System to perform a file operation on the file, wherein calling the Operating System includes providing the access identifier to the Operating System;

the step of calling the Operating System to perform an operation on the file representing the resource comprises:

assigning the access identifier to a group identifier attribute of an Operating System process, and

calling an Operating System routine from the Operating System process to perform the operation on the file representing the resource; [[and]]

granting the user access to the resource only when the Operating System call successfully performs the file operation, wherein the Operating System call successfully performs the file operation if the access identifier matches the access value;

wherein the file operation on the file representing the resource is selected from a group consisting of opening the file, closing the file, deleting the file,

reading from the file, writing to the file, executing the file, appending to the file, reading a file attribute, and writing a file attribute;

reading a permission bit associated with the file representing the resource, wherein the permission bit corresponds to a file operation performable on the file representing the resource;

based on the file operation indicated by the permission bit, determining a resource operation that is performable on the resource; and

granting the user the privilege of performing the resource operation on the resource only when the permission bit allows the file operation to be performed on the file representing the resource.

19. (original) A system as recited in Claim 18, wherein the access identifier comprises:

a first set of bits for storing a role identifier, wherein the role identifier is associated with the role; and

a second set of bits for storing the resource identifier.

20-38. (canceled)

39. (currently amended) A computer-readable storage medium, for controlling access to a resource of a plurality of resources, carrying one or more sequences of instructions which, when executed by one or more processors, causes the one or more processors to perform the steps of:

creating and storing in a filesystem of an Operating System a plurality of files that each represents a different resource of the plurality of resources;

assigning an access value to a file attribute of a file that represents the resource, wherein the file attribute is used by the Operating System to manage file access, wherein the access value corresponds to a combination of a particular role and the resource;

receiving user-identifying information from a user requesting access to the resource, wherein the user-identifying information comprises a role associated with the user, wherein the role is determined from a user identifier uniquely associated with the user and from a group identifier associated with a group that includes the user;

receiving a resource identifier associated with the resource;

creating an access identifier based on the user-identifying information and the resource identifier, wherein the access identifier is formatted as a file attribute that is used by the Operating System to manage file access;

wherein the step of creating an access identifier based on the user-identifying information and the resource identifier comprises formatting the access identifier as a group identifier file attribute;

calling the Operating System to perform a file operation on the file, wherein calling the Operating System includes providing the access identifier to the Operating System; and

wherein the step of calling the Operating System to perform an operation on the file representing the resource comprises:

assigning the access identifier to a group identifier attribute of an Operating System process, and

calling an Operating System routine from the Operating System process to perform the operation on the file representing the resource;

granting the user access to the resource only when the Operating System call successfully performs the file operation, wherein the Operating System call successfully performs the file operation if the access identifier matches the access value;

wherein the file operation on the file representing the resource is selected from a group consisting of opening the file, closing the file, deleting the file, reading from the file, writing to the file, executing the file, appending to the file, reading a file attribute, and writing a file attribute;

reading a permission bit associated with the file representing the resource, wherein the permission bit corresponds to a file operation performable on the file representing the resource;

based on the file operation indicated by the permission bit, determining a resource operation that is performable on the resource; and

granting the user the privilege of performing the resource operation on the resource only when the permission bit allows the file operation to be performed on the file representing the resource.

40. (previously presented) A computer-readable storage medium as recited in Claim 39, wherein the access identifier comprises:

a first set of bits for storing a role identifier, wherein the role identifier is associated with the role; and

a second set of bits for storing the resource identifier.

41. (canceled)

42. (previously presented) A computer-readable storage medium as recited in Claim 39, wherein the step of calling the Operating System to perform an operation on the file representing the resource comprises comparing the access identifier to an identifier included in an Access Control List file attribute associated with the file representing the resource, wherein the Access Control List file attribute includes the identifiers of all users and all groups of users allowed to access the file representing the resource.

43. (canceled)

44. (canceled)

45. (previously presented) A computer-readable storage medium as recited in Claim 39, carrying one or more additional sequences of instructions which, when executed by one or more processors, further causes the one or more processors to perform the steps of:

opening the file representing the resource;

reading from the file representing the resource a permission indicator associated with a resource operation; and

enabling the user to perform the resource operation on the resource only when the permission indicator indicates that the user is allowed to perform the resource operation on the resource.

46. (canceled)

47. (previously presented) A computer-readable storage medium as recited in Claim 39, wherein the file attribute used by the Operating System to manage file access is a group identifier file attribute.

48. (currently amended) A computer-readable storage medium, for controlling access to a resource of a plurality of resources, carrying one or more sequences of instructions which, when executed by one or more processors, causes the one or more processors to perform the steps of:

assigning an access value to a group identifier file attribute of a file that represents the resource, wherein the group identifier file attribute is used by the Operating System to manage file access, wherein the access value is uniquely determined by a combination of a particular role and the resource;

receiving a user identifier from a user requesting access to the resource, wherein the user identifier is uniquely associated with the user;

receiving a group identifier associated with a group to which the user belongs;

based on the user identifier and the group identifier, determining a role associated with the user, wherein a role identifier is uniquely associated with the role;

receiving a resource identifier associated with the resource, wherein each resource of the plurality of resources is represented by a different file stored in a filesystem of an Operating System;

constructing an access identifier on the basis of the role identifier and the resource identifier, wherein the access identifier conforms to the format of a group identifier file attribute that is used by the Operating System to manage file access;

making an Operating System call to perform a file operation on the file representing the resource, wherein the Operating System call uses the access identifier to gain access to the file representing the resource; and

granting the user access to the resource only when the Operating System call successfully performs the file operation on the file representing the resource, wherein the Operating System call successfully performs the file operation if the access identifier matches the access value;

wherein the file operation on the file representing the resource is selected from a group consisting of opening the file, closing the file, deleting the file, reading from the file, writing to the file, executing the file, appending to the file, reading a file attribute, and writing a file attribute;

reading a permission bit associated with the file representing the resource, wherein the permission bit corresponds to a file operation performable on the file representing the resource;

based on the file operation indicated by the permission bit, determining a resource operation that is performable on the resource; and

granting the user the privilege of performing the resource operation on the resource only when the permission bit allows the file operation to be performed on the file representing the resource.

49. (previously presented) A computer-readable storage medium as recited in Claim 48, wherein the access identifier comprises:

a first set of bits for storing the role identifier, wherein the role identifier represents a bitmap, each bit of the bitmap uniquely associated with a role of the user; and

a second set of bits for storing the resource identifier.

50. (previously presented) A computer-readable storage medium as recited in Claim 48, wherein the step of making an Operating System call to perform an operation on the file representing the resource comprises:

storing the group identifier value of a group identifier attribute of an Operating System process;

assigning the access identifier to the group identifier attribute of the Operating System process;

calling an Operating System routine from the Operating System process to perform the operation on the file representing the resource, wherein the operation on the file representing the resource is performed only when the value of the group identifier attribute of the Operating System process matches the value of the group identifier file attribute of the file representing the resource; and

resetting the group identifier attribute of the Operating System process to the stored group identifier value.

51. (previously presented) A computer-readable storage medium as recited in Claim 48, wherein the step of making an Operating System call to perform an operation on the file representing the resource comprises comparing the access identifier to an identifier included in an Access Control List file attribute associated with the file representing the resource, wherein the Access Control List file attribute includes the identifiers of all users and all groups of users allowed to access the file representing the resource.

52. (canceled)

53. (canceled)

54. (previously presented) A computer-readable storage medium as recited in Claim 48, carrying one or more additional sequences of instructions which, when executed by one or more processors, further causes the one or more processors to perform the steps of:

opening the file representing the resource;

reading from the file representing the resource a permission indicator associated with a resource operation; and

granting the user the privilege of performing the resource operation on the resource only when the permission indicator indicates that the user is allowed to perform the resource operation on the resource.

55. (canceled)

56. (currently amended) An apparatus for controlling access to a resource of a plurality of resources, comprising:

means for creating and storing in an Operating System filesystem a plurality of files that each represents a different resource of the plurality of resources;

means for assigning an access value to a file attribute of a file that represents the resource, wherein the file attribute is used by the Operating System to manage file access, wherein the access value corresponds to a combination of a particular role and the resource;

means for receiving user-identifying information from a user requesting access to the resource, wherein the user-identifying information comprises a role associated with the user, wherein the role is determined from a user identifier uniquely associated with the user and from a group identifier associated with a group that includes the user;

means for receiving a resource identifier associated with the resource;

means for creating an access identifier based on the user-identifying information and the resource identifier, wherein the access identifier is formatted as a file attribute that is used by the Operating System to manage file access;

wherein means for creating an access identifier based on the user-identifying information and the resource identifier comprises means for formatting the access identifier as a group identifier file attribute;

means for calling the Operating System to perform a file operation on the file, wherein calling the Operating System includes providing the access identifier to the Operating System; [[and]]

wherein means for calling the Operating System to perform an operation on the file representing the resource comprises:

means for assigning the access identifier to a group identifier attribute of an Operating System process, and

means for calling an Operating System routine from the Operating System process to perform the operation on the file representing the resource;

means for granting the user access to the resource only when the Operating System call successfully performs the file operation, wherein the Operating System call successfully performs the file operation if the access identifier matches the access value;

wherein the file operation on the file representing the resource is selected from a group consisting of opening the file, closing the file, deleting the file, reading from the

file, writing to the file, executing the file, appending to the file, reading a file attribute, and writing a file attribute;

means for reading a permission bit associated with the file representing the resource, wherein the permission bit corresponds to a file operation performable on the file representing the resource;

means for determining, based on the file operation indicated by the permission bit, a resource operation that is performable on the resource; and

means for granting the user the privilege of performing the resource operation on the resource only when the permission bit allows the file operation to be performed on the file representing the resource.

57. (previously presented) An apparatus as recited in Claim 56, wherein the access identifier comprises:

a first set of bits for storing a role identifier, wherein the role identifier is associated with the role; and

a second set of bits for storing the resource identifier.

58. (canceled)

59. (canceled)

/Tony Mahmoudi/

Supervisory Patent Examiner, Art Unit 2169